Amendments to the Claims:

This listing of claims will replace all prior versions, and listings of claims in the application. Applicant has submitted a new complete claim set Applicant has submitted a new complete claim set showing marked up claims with insertions indicated by underlining and deletions indicated by strikeouts and/or double bracketing.

Listing of Claims:

1. (Canceled)

2. (Currently Amended) A method of inviting and joining a peer to a secure peer-to-peer group comprising the steps of:

obtaining a public key (P_{U1}) of a peer;

forming, by a first member of the group, a group membership certificate containing the peer's public key (P_{U1}) and signed with a group private key (K_G)of a group public/private key pair, the group membership certificate having a structure of ((P_{U1})K_G);

sending the group membership certificate from the first member to the peer to invite the peer to join the group, the group membership certificate allowing the peer to join the group through a second member other than the first member;

receiving, at a second member of the group different from the first member, a connect message from the peer containing the group membership certificate signed by a private key of the peer, the connect message requesting connection to the secure peer-to-peer group;

the second member, authenticating the group membership certificate before allowing the peer to connect to the secure peer-to-peer group: and

if the group membership certificate is authenticated, sending an accept message to the peer including a group shared key.

3. (Previously Presented) The method of claim 2, further comprising the step of generating a group shared key to be used to encrypt group traffic.

4. (Original) The method of claim 2, wherein the step of forming a group membership certificate comprises the step of forming a group membership certificate having a structure [Version, ID, Peer ID, Serial Number, Validity, Algorithms, P_{ID}, $P_{Issuer}]K_{Issuer}$.

5. (Previously Presented) The method of claim 2, wherein the group membership certificate in the connect message from the is signed by a private key pair of the peer's public key;

when the step of authenticating is successful,

sending an accept message to the peer, and

sending a group shared key to the peer.

6. (Previously Presented) The method of claim 5, wherein the step of authenticating comprises the steps of:

verifying that at least one signature of the group membership certificate is valid;

verifying that the group membership certificate has not expired;

verifying that a hash of the peer's public key matches an identification of the peer;

opportunistically verifying ownership of the group membership certificate.

7. (Previously Presented) The method of claim 5, wherein the step of authenticating comprises the steps of:

determining if the group membership certificate is listed in a group certificate revocation list (GCRL);

determining if any certificates in a chain of group membership certificates is listed in the GCRL;

when any certificates in the chain is listed in the GCRL, determining if a date of revocation of the certificate in the chain is before a date of issue of the group membership certificate; and

when the date of revocation is after the date of issue, issuing a second group membership certificate to the peer.

8. (Currently Amended) In a secure peer-to-peer group having a predefined public/private key pair (P_G/K_G), a method of inviting a peer to join the group, comprising the steps of:

obtaining a public key (P_{U1}) of a peer by a first member of the peer-to-peer group;

forming by the first member a first group membership-certificate containing the peer's public key (P_{U1}) and a second group membership certificate signed with the group private key (K_G)~~, the first group membership certificate being~~ and signed with a private key of the first member (K_{U2}), the second group membership certificate having a structure of $((P_{U1})K_G)K_{U2}$);

sending the first and second group membership certificates from the first member to the peer to invite the peer to join the group; ~~and~~

receiving, at a second member different from the first member, a connect message from the peer containing the first group membership certificate; and

if the first group membership certificate is authenticated, sending an accept message to the peer including a group shared key.

9. (Canceled)

10. (Previously Presented) The method of claim 8, wherein the connect message from the peer contains a third group certificate comprising the first group membership certificate signed by a private key pair of the peer's public key;

authenticating the third group certificate; and

when the step of authenticating is successful,

sending an accept message to the peer from the second member, and

sending a group shared key to the peer from the second member.

11. (Previously Presented) The method of claim 10, wherein the step of authenticating comprises the steps of:

verifying that a signature of the third group certificate is valid;

verifying that the third group certificate has not expired;

verifying that a hash of the peer's public key matches a peer identification;

opportunistically verifying ownership of the third group certificate.

12. (Previously Presented) The method of claim 10, wherein the step of authenticating comprises the steps of:

determining if the third group certificate is listed in a group certificate revocation list (GCRL);

determining if either of the first and second group membership certificates is listed in the GCRL;

when either of the first and second group membership certificates is listed in the GCRL, determining if a date of revocation is before a date of issuance of the third group certificate; and

when the date of revocation is after the date of issuance, issuing a new group certificate to the peer.

13. (Currently Amended) A method of securely joining a peer-to-peer group by a peer having a public key (P_{U1}) and a private key (K_{U1}), comprising the steps of:

receiving a group invitation from a first member containing an invitation certificate ~~having~~ a group ID ~~provided therein~~, the invitation certificate including the public key of the peer (P_{U1}) signed by a private key (K_G) of the peer-to-peer group;

resolving the group ID to find a third member of the group different from the first member;

sending a connect message to the third member containing the invitation certificate signed with the private key (K_{U1}) of the peer and having a structure of $((P_{U1})K_G)K_{U1}$;

receiving an accept message from the third member containing a group membership certificate signed by a private key (P_3) of the third member; and

receiving a group shared key to enable decryption of group traffic.

14. (Previously Presented) The method of claim 13, further comprising the step of authenticating the group membership certificate signed by the private key of the third member to ensure the member's association with the group.

15. (Previously Presented) The method of claim 14, further comprising the step of resolving the group ID to find a second member of the group to which to

connect when the step of authenticating the group membership certificate signed by the private key of the third member fails.

16. (Previously Presented) The method of claim 14, wherein the step of authenticating comprises the steps of:

verifying that a signature of the group membership certificate is valid;

verifying that the group membership certificate has not expired;

verifying that a hash of the third member's public key matches a member identification;

opportunistically verifying ownership of the group membership certificate.

17. (Previously Presented) The method of claim 13, wherein the step of receiving a group invitation from a first member containing an invitation certificate having a group ID provided therein comprises the step of receiving a group invitation from the first member containing an invitation certificate and a group membership certificate; and

wherein the step of resolving the group ID to find a member of the group comprises the step of resolving the group ID to find a second member of the group; and

wherein the step of sending a connect message to the member containing the invitation certificate signed with the private key comprises the step of sending a connect message to the second member containing the invitation certificate and the group membership certificate from the first member.

18. (Currently Amended) A method of securely admitting a peer to a peer-to-peer group, comprising the steps of:

receiving at a first member of the peer-to-peer group, a connect message from the peer containing an invitation certificate generated by a second member of the peer-to-peer group and signed by a private key (K_{U1}) of the peer, the first member being different from the second member, the invitation certificate containing a public key of the peer (P_{U1}) signed by a group private key (K_G), the invitation certificate signed by the private key (K_{U1}) of the peer having a structure of $((P_{U1})K_G)K_{U1}$;

authenticating the invitation certificate signed by the peer's private key (K_{U1}); and

when the step of authenticating is successful,

sending an accept message to the peer from the first member, and

sending a group shared key to the peer.

19. (Previously Presented) The method of claim 18, wherein the step of authenticating comprises the steps of:

verifying that a signature of the invitation certificate is valid;

verifying that the invitation certificate has not expired;

verifying that a hash of a public key of the peer matches a peer identification of the peer.

20. (Previously Presented) The method of claim 18, wherein the connect message from the peer further contains a group membership certificate from the second member.

21. (Previously Presented) The method of claim 20, wherein the step of authenticating comprises the steps of:

determining if the group membership certificate is listed in a group certificate revocation list (GCRL);

when the group membership certificate is listed in the GCRL, determining if a date of revocation of the group membership certificate is before a date of issuance of the invitation certificate; and

when the date of revocation is after the date of issuance, issuing a new group membership certificate to the peer.

22. (Previously Presented) A computer-readable medium having computer-executable instructions for performing the steps of claim 2.

23. (Original) A computer-readable medium having computer-executable instructions for performing the steps of claim 8.

24. (Original) A computer-readable medium having computer-executable instructions for performing the steps of claim 13.

25. (Original) A computer-readable medium having computer-executable instructions for performing the steps of claim 18.